TCIPG

ANNUAL INDUSTRY WORKSHOP
NOVEMBER 12-13, 2014

SECURITY OF CLOUD COMPUTING FOR THE POWER GRID

NOVEMBER 12 -13, 2014

DAVID L. NORTON, CISSP

FEDERAL ENERGY REGULATORY COMMISSION
SENIOR CRITICAL INFRASTRUCTURE PROTECTION ADVISOR

FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T

COMMENTARY FRAME OF REFERENCE

- Thoughts are mine alone; not FERC's…
- 30+ years buying, building, operating, maintaining, advising, vending and supporting Clouds / services; both public and private
- My focus is on the BPS – "Transmission" per se
- Situational awareness / command & control
- Interstate domestic national security criticality!
- Mission obliged to faithfully serve the 'public trust'

POSITION: NOT FOR CRITICAL C&C NETWORKS

- Opaque! Poor choice for situational awareness / C&C
- Are you comfortable relinquishing control?
  - Performance engineering (availability / throughput)
  - Security – confidentiality, and therewith potentially integrity
  - Location – OCONUS countries claim data ownership // FIPS140
  - Virtual – CIPv5 device level security, not HyperV /instance /circuit
  - Agility – ability to quickly respond to outages/urgent change
  - Do you *know* vendor security solution is better; better staff?
- There can be significant differences between vendor promise and performance; only *eventual* recourse for bad performance is the legal system. Not real time…
- One can delegate responsibility, but never accountability!

RECOMMENDATION: ROLL YOUR OWN…

- Cloud services attraction: To save money. Maybe.
- Build a private cloud: Done capably will cost less to procure/implement, O&M; especially monthly Telco
- EASEMENT !!! Huge financial advantage…
- A few very good really well paid network engineers…
- ‘Hands-on’ work rolled into asset management O&M
- And most of all, you KNOW what’s going on in your network; control your own fate as much as possible

PARTING SHOTS…

1) Natural evolution has created mankind with an innate, dare say healthy, fear of the unknown. Fine, except when taken to extreme. Since secure high-performance data network engineering is not often an organizational core competency, it's usually assumed that some other company can do it better, and cheaper… Yet, utilities run the most complex machine in the world, with dire consequence for failure and sloth in recovery… Don't be too quick to outsmart yourself – Don't rationalize away the 'loss of control' while at the same time still having fiduciary 'accountability.'

PARTING SHOTS…

2) How will you know if you are indeed “getting a deal” on a Cloud service, even disregarding ‘loss of control’ and ‘accountability’ factors, if first you have not yourself (even with help) implemented an effective solution set? Only then will you know what fair procurement and build costs are…

3) After 18 months(+) of steady state operation, even with help, bid-out a long term O&M “in-sourcing” support contract. Experience gained will allow decent estimation of ongoing future data net operating costs.